



**STRATEGY  
RESEARCH  
PROJECT**

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

**INFORMATION OPERATIONS:  
COUNTERING THE ASYMMETRIC THREAT TO  
THE UNITED STATES**

**BY**

**LIEUTENANT COLONEL (P) WENDELL B. McKEOWN  
United States Army**

**DISTRIBUTION STATEMENT A:**

**Approved for public release.**

**Distribution is unlimited.**

19990601 060

**USAWC CLASS OF 1999**



**U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050**

USAWC STRATEGY RESEARCH PROJECT

**Information Operations: Countering the Asymmetric  
Threat to the United States**

by

LTC(P)Wendell B. McKeown  
United States Army

COL Ralph Ghent  
Project Advisor

The views expressed in this academic research paper are those of the author and do not necessarily reflect the official policy or position of the U.S. Government, the Department of Defense, or any of its agencies.

DISTRIBUTION STATEMENT A:  
Approved for public release.  
Distribution is unlimited.

U.S. Army War College  
CARLISLE BARRACKS, PENNSYLVANIA 17013



## **ABSTRACT**

AUTHOR: LTC(P) Wendell B. McKeown

TITLE: Information Operations: Countering the Asymmetric  
Threat to the United States

FORMAT: Strategy Research Project

DATE: 7 April 1999 PAGES: 39 CLASSIFICATION: Unclassified

The United States is dependent on information. As we move into the 21<sup>st</sup> Century our reliance on information systems will only increase. The cornerstone of Joint Vision 2010 is information superiority. Every facet of future military operations will be critically linked to an aggregate cyber network that relies on critical national infrastructures to provide for information superiority. This 'system of systems' is vital in performing both routine and crisis action military activities. Our dependence on this infrastructure places the United States in a highly vulnerable position to asymmetric attacks. This paper will examine the impact on our military if it were unable to effectively communicate and coordinate. It examines the vulnerabilities of the information infrastructure and argues that recent national policy changes will be effective in dealing with the threats to both civil and military operations.



## TABLE OF CONTENTS

ABSTRACT .....	iii
DEFINITIONS .....	3
TODAY'S INFORMATION ENVIRONMENT .....	5
THE CHALLENGE .....	7
THE TARGETS .....	8
THE ENEMY .....	11
A POSSIBLE SCENARIO .....	13
RESPONDING TO THE THREAT .....	16
RISKS .....	21
CONCLUSION .....	23
ENDNOTES .....	27
BIBLIOGRAPHY .....	31



We know with specificity of several nations that are working on developing an information warfare capability. It is clear that nations developing these programs recognize the value of attacking a country's computer systems both on the battlefield and in the civilian arena. If we overlook this point and simply rely on building of a costly army ... it is just as good building a contemporary Maginot Line. These countries recognize that cyber-attacks ... against civilian computer systems in the US represent the kind of asymmetric option they need to 'level the playing field' during an armed crisis against the United States.

—CIA Director George Tenet

Much has been written about cyber war, hacking, and other high tech 'doomsday' scenarios. This paper will focus on Information Operations in the context of cyber and kinetic warfare and the measures necessary to defend against them. It will define the terms associated with Information Operations, identify potential targets, and illustrate examples of possible Information Operations scenarios. Finally, it will argue that recent civil and military policy changes have enhanced our ability to win the information war by gaining and maintaining information superiority.

In 1996, the Chairman of the Joint Chiefs of Staff published Joint Vision 2010(JV 2010). This publication established a vision for how the U.S. military will fight in the uncertain future of the 21<sup>st</sup> century.

Four operational concepts were introduced in JV 2010. These concepts, as one author wrote "if mastered, will allow the U.S. military to engage in "decisive operations" and succeed at any mission and at any level of war."<sup>1</sup> The four operational concepts introduced in JV 2010 that will enable the U.S. to achieve "full spectrum dominance" are "dominant maneuver," "precision engagement," "full dimensional engagement," and "focused logistics." The essential enabler for all four of these concepts is "information superiority."<sup>2</sup>

Information superiority is the cornerstone of Joint Vision 2010. The United States military is dependent on information, and ultimately the infrastructure supporting information flow. Information is vital to our everyday existence. It is especially critical to our ability to prepare, deploy, command, and control forces during military operations and crisis. Because of decreased defense budgets, downsizing, and commercialization we no longer have the luxury of a dedicated military communications network. For the first time in history, the Department of Defense is critically dependent upon an infrastructure that it neither controls nor influences. Our environment is one that is heavily reliant upon commercial systems to interface the National, Global and Defense information infrastructures. This aggregate network renders the whole vulnerable. An attack, either cyber or physical, on any

portion could seriously hamper military operations even before the first shot is fired.

The intense reality is Information Operations are a viable instrument of war for a wider range of potential adversaries; much broader than that field of kinetic players. Information Operations represents one instrument that could indeed 'level the playing field' for any competitor to gain an advantage over the U.S. military. Even lesser, non-state actors could leverage Information Operations to their advantage. This concept is best stated by the famous military writer and tactician Sun Tzu, who wrote "In battle one engages with the orthodox and gains victory through the unorthodox."<sup>3</sup>

The nuclear age forced America to develop new national policies focused on defending itself from the nuclear threat. With the emergence of an Information Warfare threat, the same need exists for new national policies to defend the U.S. against the Information Operations threat. Recent policy and organizational changes signal that the U.S. has indeed recognized the Information Operations threat and is taking prudent measures to defend against the cyber threat.

## **DEFINITIONS**

In order to better understand terms and concepts used in this paper the following discussion of terminology is provided.

Joint Vision 2010 defines information superiority as "the capability to collect, process, disseminate an uninterrupted flow of information, while exploiting or denying an adversary's ability to do the same. Information superiority will require both offensive and defensive Information Warfare (IW)."<sup>4</sup>

A sub-set of Information Superiority is information assurance. Information assurance is defined as "information operations that protect and defend information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation."<sup>5</sup> "This includes providing restoration of information systems by incorporating protection, detection, and reaction capabilities."<sup>6</sup>

Information Operations is defined as an "action taken to affect adversary information and information systems while defending one's own information and information systems."<sup>7</sup>

Offensive information warfare will "degrade or exploit an adversary's collection or use of information. It includes both traditional methods, such as a precision attack to destroy an enemy's command and control (C2) capability, as well as nontraditional means such as electronic intrusion into an information and control network to convince, confuse, or deceive."<sup>8</sup>

Defensive Information Operations "ensure timely, accurate, relevant information access while denying adversaries the

opportunity to exploit friendly information and information systems for their own purposes."<sup>9</sup> Additionally, "traditional defensive Information Warfare operations include physical security efforts and encryption. Nontraditional methods will range from anti-virus protection to new innovative means for secure data transmissions."<sup>10</sup>

### **TODAY'S INFORMATION ENVIRONMENT**

America is firmly entrenched in the 'Information Age.' The advantages of technology have created information dependence. The average American needs only to look around their home and work place to view how information technologies have changed his life. Cellular telephones, paging, the Internet, Automatic Teller Machines (ATM) and instantaneous television coverage all have contributed to the information revolution and our dependence on information.

The military has also become increasingly reliant on information technologies. We have increasingly relied on leveraging technology to gain advantages in weapons, systems, C2, and intelligence. Our military's performance is critically linked to information and information systems."<sup>11</sup>

Joint Pub 3-13 best describes the current information environment by stating, "The labels placed on information systems and associated networks may be misleading as there are

no fixed boundaries in the information environment. Open and interconnected systems are coalescing into a rapidly expanding global information infrastructure (GII) that includes the US national information infrastructure (NII) and the DII."<sup>12</sup>

The GII is "the world wide interconnection of communications networks, computers, data bases, and consumer electronics"<sup>13</sup> that allows information to be available to users.

The National Information Infrastructure (NII) is similar in nature and purpose to the GII but relates in scope only to the national information environment, which includes all government and civilian information infrastructures.<sup>14</sup>

The second part comprising the National Information Infrastructure is the Defense Information Infrastructure (DII). The DII is deeply embedded and integrated into the NII. This seamless relationship makes distinction between them difficult. The DII is a shared and interconnected system of computers, communications, applications, security, people, and other support structures serving DOD local, national, and worldwide needs. The DII connects DOD mission support, Command and Control (C2), and intelligence computers through voice, telecommunications, imagery, video, and other multimedia services via the Defense Information Systems Network (DISN). It includes C2, strategic, tactical, intelligence, and commercial

communications systems and facilities to transmit DOD information.<sup>15</sup>

## **THE CHALLENGE**

The successful conduct of military operations requires access to information availability both inside and outside the 'operational' area. It must be available for pre-deployment, deployment and during operations. Modern command structures require frequent, instant and reliable access to information at locations in the continental United States as well as forward-deployed theaters.

Because of this paradigm shift, information infrastructures no longer parallel traditional command lines. Additionally, our reliance on commercial providers have 'blurred' the distinction between commercial and military system access and control.

Primary examples of the dependence on commercial systems are the Battlefield Operating Systems (BOS) of mobility and sustainment of forces. Both of these systems are almost totally dependent on commercial infrastructures. They rely on international telecommunications, the public switched network, commercial satellites and ground stations, transportation systems, and the electric power grid.<sup>16</sup> This dependency is best symbolized by the fact that approximately 95% of all military communications are routed through commercial facilities.<sup>17</sup>

## THE TARGETS

Joint Pub 3-13 identifies four broad categories of Information Operations targets. They are leadership, military infrastructure, civil infrastructure and weapons systems. For the purpose of this paper the focus will be on the military and civil infrastructure aspects of Information Operations targeting.

Robert Steele adds more clarity to Information Operations targeting as he describes in his paper, Takedown: Targets, Tools, and Technology, four sub-categories of vulnerability of the civil and military infrastructures. He categorizes them as: Major Physical Infrastructure elements, key military/civil facilities and infrastructure, core data systems vital to national security and the intelligence community network.<sup>18</sup>

Physical infrastructure targets include a wide array of targets including over 2800 bridges, levees, and dams, of which approximately 200 are of strategic importance. The two major rivers in the United States, the Mississippi and the Missouri, have only six major rail bridges spanning them. The loss of any or all would have devastating effects on commerce and military transportation traversing the United States, coast-to-coast.<sup>19</sup>

Also included are dams, which present a unique target in that they are susceptible to both cyber and physical take-over to either release water or stop the flow to destroy the facility

while disrupting transportation, electricity production, and generally creating havoc.

Canals are also included in this category. A primary example being the Panama Canal. This facility, though not located within the US, is vital to our ability to project forces. Its loss through cyber or physical takedown would be catastrophic to both military and commercial endeavors and would serve to be a major military, as well as economic, "choke point."<sup>20</sup>

United States pipelines such as the Alaskan pipeline are critical and are highly vulnerable targets as well. This pipeline goes across vast uninhabited areas and carries over 10% of the domestic oil for the U.S.

Additionally, critical railway switching points are essential elements for transportation and are highly vulnerable and relatively unprotected. Such a center is the Cincinnati rail yards. This facility possesses the only major turnstile for re-orienting rail cars in the US. Its destruction would virtually paralyze rail operations in the U.S.

A second category of vulnerability is, as Robert Steele refers to them, the "military Achilles' heels."<sup>21</sup> Specific commercial sites directly and indirectly supporting military operations are highly lucrative targets as well. These include civilian power and communications nodes supporting command

centers and other important facilities. Examples of these include the commercial Electronic Switching System (ESS), military data switches such as the Culpepper Switch and commercial Internet switches such as the MAYEAST and MAYWEST nodes. The cyber and/or physical destruction of these facilities and their capabilities would grind the military C2 process to a halt.<sup>22</sup> The ability of forces to mobilize and deploy, and once deployed, to use information via 'reach back' is deemed another vulnerability. Facilities housing satellite downlink equipment, power generation and telecommunications processing centers are also targets.

These targets include essential communications nodes such as the Navy antenna fields located at the Annapolis golf course and satellite downlink stations at Fort Belvoir and at the Alternate National Military Command Center near the former Fort Ritchie in Maryland.

The third area of concern involves the national databases. These targets include historical, environmental, and other critical planning data, including air traffic control and rail car control. Additionally, data such as fuel stockage levels, military logistics data, transportation systems and financial data are included in this category.<sup>23</sup>

Another primary target will be the DOD computer network. A 1998 Joint FBI and Computer Security Institutes (CSI) survey

revealed that computer crime and security breaches have increased by over 16% since 1997 and that attacks against the Department of Defense computer systems have increased substantially.<sup>24</sup>

The final area of concern is the intelligence community. Cyber or kinetic attacks against the vulnerable sites at the National Security Agency, Fort Belvoir, Defense Intelligence Agency sites at Suitland Maryland and Bolling Air Force Base could severely hamper and ultimately 'blind' our intelligence efforts. These sites, along with countless others, are in the public view and are openly vulnerable to direct physical attack from outside the 'fence line.'<sup>25</sup>

In summarizing the asymmetric infrastructure vulnerabilities of the United States Robert Steele writes:

a "takedown" of America is not simply a matter of electronic attacks against electronic systems, but rather a much more comprehensive range and scale of vulnerability which encompasses everything from key geo-physical nodes to our intelligence mind-sets, and which can be attacked with a range of tools that includes: pick axes and chain saws against selected cables; anti-tank missiles against AWACS ... satellites dishes; 18 wheeler trucks with and without explosives against specific transformers or other key nodes; electric attacks; ...<sup>26</sup>

## **THE ENEMY**

One of the most disturbing aspects of the post cold war era is the difficulty in identifying the threat. As we move into

the information age of warfare, the cast of potential enemies is unlimited. The 'threat set' is composed of a diverse group of potential actors. They include nation state actors, fundamentalist religious groups, hackers, vandals, criminals, terrorists and angry insiders.<sup>27</sup>

Their reasons for attack are as varied as their backgrounds and interest. Their motives range from fanatical religious zealots desiring to send a holy message to the world to political moralists who want to display they power and influence. Other motives for attack include monetary gain orientation and intelligence gathering efforts. The fact is few if any nations can challenge the United States using traditional force-on-force. Information warfare is cost effective, and offers a non-attribution capability that can be totally hidden during development and deployment.

Major General Robert Scales, in writing about the future adversaries of the US, states that future opponents will "heed the lessons of the Gulf War and will ... design a strategy that avoids our strength and uses indirect means to erode our national will ... this opponent will exploit American weaknesses such as over reliance on technology..."<sup>28</sup>

Looking toward 2010, US Forces will rely heavily on leveraging of technology for information dominance and superiority increased lethality and survivability. Forces will

be lighter, more tailorable and more reliant on communications systems hosted by the private sector. The nature of the threat can be characterized by "attack and disruption not just by states but also non-state actors, terrorist groups, and even individuals."<sup>29</sup> Experts predict the Information Operations threat will increase exponentially. It will only diminish, they say, with solutions such as early warning/detection and physical security measures, many of which are commercially available now.<sup>30</sup>

In summary, the diverse nature of the potential threats, coupled with fiscal restraint and lack of public interest, makes defense of the National Information Infrastructure a challenge.

### **A POSSIBLE SCENARIO**

0300Z 24 July 1999, North Korea commences offensive operations and crosses the 38<sup>th</sup> Parallel. The Commander, United States Forces Korea, implements his operations plan. Based on the timed phased force and deployment data (TPFDD), Headquarters, III US Corps receives alert notification and begins recall and notification of subordinate units. These units include the 1<sup>st</sup> Cavalry Division and the 4<sup>th</sup> Infantry Division, both stationed at Fort Hood.

At 0600Z, one of two Texas Power and Light (TPL) power grid relay stations servicing Fort Hood is knocked out as a result of

a 'drunk' driver crashing his pickup truck into the facility. Power to over one-half the post, including the 1<sup>st</sup> Cavalry Division area, is affected.

One hour later at 0700Z, a highly suspicious fire occurs in the SPRINT ESS switch providing telephone service to Fort Hood. Investigators at the site report the fire to be an act of arson. The result is no telephone service within the greater Fort Hood area. Consequently, unit recalls and essential C2 operations are degraded, slowing the muster and coordination efforts of the units.

Nearly simultaneously to the fire, a civilian commercial ammunition hauler crashes an 18 wheeler into the Robert Gray Army Airfield (RGAAF) Air Traffic Control terminal at West Fort Hood. Air Traffic Control services are degraded but the airfield is still operational until the local navigation and guidance air traffic control radar is forcibly powered down through a remote computer entry. Because of this series of events, RGAAF is 'blind' and is therefore incapable of receiving or launching air traffic.

Due to the power outage encountered at Fort Hood the local rail switch is incapable of moving rail cars and to facilitate rail movement from Fort Hood. Additionally the servicing rail line reports that 'computer problems' associated with its rail switching center at Cincinnati, Ohio is interfering with its

ability to route locomotives and rail cars to the central Texas area.

Meanwhile, at the seaport of embarkation, Beaumont, Texas, a massive power outage has occurred as a result of the failure of its central computer system. The failure is reported to have been caused by insider hacking efforts and the planting of a time-delayed shutdown command to the power grids. Consequently the port is completely shut down and is incapable of loading, unloading, or controlling shipping in or out of the port.

At 1000Z, the Director of Information Management (DOIM) at Fort Hood reports that 'spamming' efforts have effectively clogged the NIPRNET/Internet gateway. He requests permission to impose 'minimize' and limit Internet access by on-post personnel. Minimize is subsequently authorized and placed into effect. However, a replicating e-mail virus previously received by a post e-mail recipient begins flooding the post's e-mail network, effectively disabling it.

By 1200Z, the North Korean advance into South Korea is rapidly progressing. Meanwhile, Republic of Korea forces and the United States 2<sup>nd</sup> Infantry Division are inflicting heavy casualties and slowing the attack. The Commander, USFK reports that his forces are capable of slowing the attack but will require reinforcement within 48 hours to blunt and stop the attack.

The Joint Chiefs of Staff reports to the Chairman that due to kinetic and cyber attacks, III Corps will be unable to deploy and reinforce for at least 72 hours.

0200Z 26 July 1999, North Korean forces enter Seoul and proceed southward. At 1000Z 26 July 1999, Republic of Korea forces are rendered combat ineffective and ultimately surrender. US forces continue to fight and ultimately are evacuated via air and sea.

South Korea has fallen, not as a result of the massive North Korean invasion, but from a group of less than 20 individuals attacking the critical civil/military infrastructure of the United States.

The example provided in this scenario, though fictional, represents a very likely scenario for the future of warfare. A small, highly skilled and organized group using both kinetic and cyber means could effectively stop military operations. It graphically portrays a potential glimpse into the future in that any or all of these actions could drastically affect the consequences of a military action, a military action reliant on commercial means to accomplish the mission.

## **RESPONDING TO THE THREAT**

Before July 1996 the U.S. Government policy regarding critical infrastructure protection had been only loosely defined

and was poorly organized. Essentially the United States had no comprehensive national policy on information warfare, assurance, or information protection.<sup>31</sup>

The initial step in responding to the emerging threat of cyber war was the Presidents Council on Critical Infrastructure Protection (PCCIP). The commission was established by Executive Order 13010 in July 1996. It was created to coordinate and recommend initiatives and legislation for the protection of the critical infrastructure. The PCCIP used, as it's charter that,

Information itself has become a strategic national asset and the maintenance and protection of our information systems has become a vital national interest of the United States. Our dependence upon information technologies and the global connectivity of today's information systems result in a new strategic threat aimed at those information systems that control essential aspects of our military, economic, and political power.<sup>32</sup>

The PCCIP performed a valuable service to the nation. It focused the debate on critical infrastructure protection and reinforced the concept of the cyber world and its connection to defense and economic security. It categorized the threats to the critical infrastructure as physical and cyber, and called for cooperation between the private and government sectors to develop strategies to protect the infrastructure. The PCCIP was instrumental in the President drafting Presidential Decision Directive (PDD) 63, the Critical Infrastructure Protection Directive.

Before PDD 63, responsibility for information infrastructure security was spread over numerous boards, commissions, working groups and advisory councils throughout the executive branch with no designated lead agency or department in charge.<sup>33</sup>

Responding to the findings and recommendations of the PCCIP and various other organizations including the Defense Science Board, Quadrennial Defense Review (QDR) and the National Defense Panel (NDP), the Clinton administration produced PDD 63.

The general guidelines of PDD 63, The Critical Infrastructure Protection Directive, call for "a national effort to assure the security of the increasingly vulnerable and interconnected infrastructures of the United States."<sup>34</sup>

The most critical aspect of PDD 63 is that for the first time the President identified critical infrastructure protection and cyber-security as a national security issue.<sup>35</sup> The directive requires immediate federal government action including risk assessment and planning to reduce exposure to attack.

It stresses the critical importance of cooperation between the government and the private sector by linking designated agencies with private sector representatives. The directive sets a goal of a reliable, interconnected, and secure information system infrastructure by the year 2003. Additionally, it requires significantly increased security for all government systems by 2000.

In addition, PDD 63 establishes a national center to warn of and respond to attacks and establishes a new structure to deal with this important challenge. The structure includes a National Coordinator whose scope is not only infrastructure security, but also foreign terrorism and threats of domestic mass destruction.

Presidential Decision Directive 63 calls for the National Infrastructure Protection Center (NIPC) at the Federal Bureau of Investigation (FBI) to serve as a fusion center. This fusion center consists of representatives from the FBI, Department of Defense, United States Secret Service, Department of Energy, and Transportation, the Intelligence community and the private sector. Furthermore it designates the NIPC as the principal for coordinating the Federal Government's response to an incident, mitigating attacks, investigating threats and monitoring reconstitution efforts, and establishes the National Infrastructure Assurance Council (NIAC).

The NIAC is a panel composed of private sector and state/local governments which will provide policy input to the national strategy.

The directive establishes the Critical Infrastructure Assurance Office (CIAO) within the Department of Commerce. Its responsibilities include creating capabilities, technologies and skills for national protection. The CIAO is envisioned to be

the primary planning element supporting the National Coordinator, the Secretary of Commerce, and is responsible for coordination efforts between government agencies and the private sector. This office is also responsible for coordinating national education and awareness programs as well as legislative and public affairs.<sup>36</sup>

Most recently, on 22 January 1999, President Clinton announced that he would allocate in his FY 2000 budget \$1.46 billion dollars to "defend our critical infrastructure, including, power generation systems, banking, transportation and emergency services and telecommunications."<sup>37</sup> Included in his proposal was funding for research and development to safeguard key computer systems, with a focus on developing tools that can identify potentially threatening activities.

The establishment of the Joint Task Force on Computer Network Defense (JTF-CND) in December 1998 signaled the Department of Defense's commitment to countering threats against Department of Defense networks and computer systems. The JTF-CND will serve as the focal point with the Department of Defense to organize a united effort to defend its computer networks and systems. It will monitor incidents and potential threats to DoD systems. It will also establish links with other federal agencies through the NIPC to share information on activities across the information infrastructure.

When attacks are detected, the JTF will be responsible for directing DoD-wide recovery actions to stop or contain damage and restore network functions to DoD operations. Currently the JTF reports through the Chairman of the Joint Chiefs of Staff to the Secretary of Defense since the joint task force is not assigned to a unified command. It will be assigned to United States Space Command on 1 October 1999. Joint Task Force-Computer Network Defense is located at and supported by the Defense Information Systems Agency (DISA).<sup>38</sup>

Other positive signs that the Department of Defense has embraced Informational Operations are the creation of an officer Functional Area (FA) for Information Operations. This FA was established under Officer Personnel Management System XXI (OPMS XXI) to manage Information Operations for the warfighting CINC.

Additionally the creation, and subsequent growth, of the Land Information Warfare Agency (LIWA) and Computer Emergency Response Teams (CERT) all point to the Department of Defense commitment to ensuring critical infrastructure protection and information superiority.

## **RISKS**

As positive as all of these initiatives are there are risks associated with protection of the critical infrastructure and to our ability to gain and maintain information superiority. These

risks are not those associated with the potential enemy threat. These risks are internal. One of the greatest being the critical need for support of information security funding. In 1998, the Presidents Commission on Critical Infrastructure Protection recommended \$250 billion in research and development funding for assurance technologies.

In the 1999 budget, the Department of Defense requested nearly \$70 billion for information assurance. The House National Security and Appropriations Committee fully funded the request, while the Senate Armed Services Committee reduced that amount to \$30 billion. Meanwhile, the Senate Appropriations Committee zeroed out the entire 'line'.<sup>39</sup> Some writers have concluded that the public, as well as Congress, does not view the cyber threat as creditable. Others say that it may take an 'electronic Pearl Harbor' to put teeth in the strategy and gain wide spread support for increased funding.<sup>40</sup>

The high cost of critical infrastructure protection is also a risk to information assurance. Infrastructure protection will not be cheap. Computer network defense measures are relatively low cost measures when compared to hardening and construction of redundant systems and facilities to ensure both cyber and physical security.

Another high-risk area for critical infrastructure protection is the need for cooperation between commercial,

government and military elements on protection standards and priorities. Due to our reliance on commercial systems for Department of Defense and other governmental information systems, we will be forced to lead the effort from 'behind' and gain consensus versus regulation.

Public interest and concern for critical infrastructure protection and information assurance is another area of concern. Even with the current discussion and preparation for the year 2000, it is unclear if the American public is willing to divert tax dollars to infrastructure hardening and protection without a major incident to draw their attention to its importance.

## **CONCLUSION**

The threat described in this paper is not limited as only a tool against our military. It is a national threat that must be dealt with by all the national assets. It must be viewed with an eye toward a totally integrated defensive and offensive information assurance plan. The foundation of this integrated plan lies in the roots of the President Commission on Critical Infrastructure Protection and Presidential Decision Directive 63 and the off shoots of the Presidential Decision Directive. The DII, NII and GII are an integrated system of systems, which are only as strong as the weakest link. As discussed earlier, a 'takedown' of the United States may not be by hacking or

electronic attack alone. A 'takedown' may be attempted by a combination of means ranging from less sophisticated kinetic means to a major cyber attack on our national/military systems, or a combination of both means.

Undoubtedly PDD 63 was a major step in filling a critical void that has existed in the United States national security policy. The directive's simple act of identifying information infrastructure protection as a national security issue is a monumental achievement. It formally identified an emerging threat that many fear will become the opening shots of World War III. Presidential Decision Directive 63 along with the National Security Strategy is a sound foundation that clearly defines roles, missions, and responsibilities. It defines the threat and establishes a sound structure to respond to potential threats and attacks along with developing early warning and detection capabilities. The directive's near term value is unquestionable and has been viewed by most observers as a positive step in the right direction.<sup>41</sup> There is virtual unanimous support and praise for the administration's efforts in PDD 63.

Joint Vision 2010 relies on information superiority to enable the operational aspects of dominant maneuver, precision engagement, full-dimensional protection and focused logistics. Our military relies on its backbone communication infrastructure

to coordinate, command, control, deploy and force project. Information assurance will be vital to the success of JV 2010. Our national military effort is inextricably linked to the critical national infrastructure. The foundation laid by PDD 63, prompted the establishment of a network of organizations which will be capable of strengthening protection of our critical nation information infrastructure.

The PCCIP, PDD 63, the Joint Task Force for Computer Network Defense, along with other federal organizations recently established are all positive indications that we recognize the threat and are applying a multifaceted information assurance plan into operation. We are applying resources to counter the threat and are poised to respond in order to protect this vital national interest of information.

We must continue efforts to harden, protect, provide redundancy, and enhance physical and cyber security. More importantly, we must incorporate civilian sector informational and other infrastructure facilities within the 'umbrella' of the NII.

Without this multi-faceted approach, our ability to respond to an adversary will be severely hampered, and will place our nation in peril, both militarily and economically.

Information has become a strategic national asset. The maintenance and protection of our information systems and

infrastructure has become a vital national interest. We have only recently addressed the emerging threat to our Informational Infrastructure and developed a strategy to deal with that threat. Our challenge is to adapt our strategy to the emerging threats more quickly than potential attackers. Our nation must continue to reevaluate and execute the comprehensive National infrastructure protection strategy to guarantee information assurance and information superiority now and into the 21<sup>st</sup> Century.

WORD COUNT = 4,989.

## ENDNOTES

<sup>1</sup> Sam Cox et al., "Information Assurance - the Achilles' Heel of Joint Vision 2010?," Joint Staff Information Assurance Digest 80 (August 10 1998); 2.

<sup>2</sup> Joint Chiefs of Staff, Joint Vision 2010, (Washington D.C., Government Printing Office, July 1996), 69.

<sup>3</sup> Sun Tzu, The Art of War, translated by Ralph D. Sawyer, (Boulder Colorado, Westview Press, 1994), 187.

<sup>4</sup> Joint Vision 2010, 66.

<sup>5</sup> Ibid., GL-7

<sup>6</sup> Ibid.

<sup>7</sup> Ibid.

<sup>8</sup> Joint Vision 2010, 66.

<sup>9</sup> Joint Chiefs of Staff, Joint Doctrine for Information Operations, Joint Pub 3-13, (Washington D.C., Government Printing Office, 9 October 1998), I-9.

<sup>10</sup> Joint Vision 2010, 66.

<sup>11</sup> Peter J. Farrell, "A National Security Strategy for Information Assurance" (US Army War College Strategic Research Project, 1997), 6.

<sup>12</sup> Joint Pub 3-13, I-13.

<sup>13</sup> Ibid.

<sup>14</sup> Ibid., I-14.

<sup>15</sup> Ibid., I-14.

<sup>16</sup> Ibid., I-15.

<sup>17</sup> David S. Alberts and Daniel S. Papp, Information Age Anthology, Volume 1, Part Three, "Government and the Military" (National Defense University, June 1997) 524.

<sup>18</sup> Lloyd J. Matthews, ed., Challenging the United States Symmetrically and Asymmetrically: Can America be Defeated? (Carlisle Barracks, Pa., 1998), 121-122.

<sup>19</sup> Ibid., 124.

<sup>20</sup> Ibid., 125.

<sup>21</sup> Ibid., 122.

<sup>22</sup> Ibid., 125.

<sup>23</sup> Ibid., 126.

<sup>24</sup> Computer Security Institute, Computer Security, Issues & Trends, Vol. IV, No.1, Winter 1998, 1.

<sup>25</sup> Matthews, 126.

<sup>26</sup> Ibid., 127.

<sup>27</sup> U.S. Department of the Army, Information Operations, Field Manual 100-6, Washington D.C., 1-6.

<sup>28</sup> Robert H. Scales, America's Army: Preparing for Tomorrow's Security Challenges, Army Issue Paper No. 2, U.S. Army War College, Carlisle, Pa., 6.

<sup>29</sup> Roger C. Morlander, Andrew Riddle, and Peter A. Wilson, Strategic Information Warfare: A New Face of War", Parameters. (August 1996): 85.

<sup>30</sup> George Seffers, "Jeffrey Hunker: Chief of Critical Infrastructure Assurance Office," The Army Times, 12 October 1998, 30.

<sup>31</sup> The Joint Chiefs of Staff, and the National Defense University, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, 2<sup>nd</sup> Edition (Washington: US Government Printing Office), 1-1.

<sup>32</sup> Farrell, iii.

<sup>33</sup> Ibid.

<sup>34</sup> The White House, Presidential Decision Directive 63, "Critical Infrastructure Protection", May 1998; available at <http://www.pub.whitehouse.gov/uri-res/12r?urn:pdi//oma>. Internet accessed 29 January 1999.

<sup>35</sup> Ibid.

<sup>36</sup> Ibid.

<sup>37</sup> Critical Infrastructure Assurance Office Press Release, dated January 14 1999, "President Clinton and Vice President Gore: Keeping America Secure for the 21<sup>st</sup> Century" available at <http://www.ciao.gov/tpjan22.html>. Internet accessed 29 January 1999.

<sup>38</sup> Office of the Assistant Secretary of Defense (Public Affairs) Press Release, dated 30 December 1998, "Joint Task Force on Computer Network Defense Now Operational" available at <http://www.defenselink.mil/cgi-bin>; Internet accessed 2 January 1999.

<sup>39</sup> Seffers, 30.

<sup>40</sup> Farrell, 24.

<sup>41</sup> Ibid., 30.



## BIBLIOGRAPHY

- "A Prelude to Info-War?", Wired News, Reuters, (24 June 1998)  
Available from <<http://www.wired.com/news>>; Internet  
accessed 30 Dec 1998.
- Alberts, David S. and Daniel S. Papp, eds. The Information Age:  
An Anthology on its Impacts and Consequences. Vol.1, Part  
Three: Government and the Military. Fort Lesley J. McNair,  
Washington D.C.: National Defense University, June 1997.
- Bunker, Robert J., "Information Operations and the Conduct of  
Land Warfare", The Land Warfare Papers, No. 31, Institute of  
Land Warfare, Association of the United States Army,  
Arlington, Virginia (Oct 1998).
- Cole, John C., "Fighting Cybercrime", Military Review, (March-  
April 1998) Available from <[http://www-  
cgsc.army.mil/milrev/english/marapr98/coale.htm](http://www-cgsc.army.mil/milrev/english/marapr98/coale.htm)>; Internet  
accessed 30 Dec 1998.
- Computer Security Institute, Computer Security, Issues & Trends,  
Vol. IV, No.1, Winter 1998
- Cox, Sam, Ron Stimeare, Tim Dean, and Brad Ashley, "Information  
Assurance - the Achilles' Heel of Joint Vision 2010?", Joint  
Staff Information Assurance Digest, Edition 80 (August 10  
1998): 1-12.
- Critical Infrastructure Assurance Office Press Release, dated  
January 14 1999, "President Clinton and Vice President Gore:  
Keeping America Secure for the 21<sup>st</sup> Century" available at  
<<http://www.ciao.gov/tpjan22.html>>; Internet accessed 29  
January 1999.
- Farrell, Peter J., "A National Security Strategy for Information  
Assurance" (US Army War College Strategic Research Project,  
1997)
- Matthews, Lloyd J., ed. Challenging the United States  
Symmetrically and Asymmetrically: Can America be Defeated?.  
Carlisle Barracks. Pa.: Strategic Studies Institute, U.S.  
Army War College, July 1998.
- Morlander, Roger C., Andrew Riddle, and Peter A. Wilson,  
Strategic Information Warfare: A New Face of War,  
Parameters. (August 1996)

Office of the Assistant Secretary of Defense (Public Affairs)  
Press Release, dated 30 December 1998, "Joint Task Force on  
Computer Network Defense Now Operational" available at  
<<http://www.defenselink.mil/cgi-bin>>; Internet accessed 2  
January 1999.

The White House, Presidential Decision Directive 63, "Critical  
Infrastructure Protection", May 1998 available at  
<<http://www.pub.whitehouse.gov/uri-res/12r?urn:pdi//oma>>;  
Internet accessed 29 January 1999.

Tzu, Sun, The Art of War, translated by Ralph D. Sawyer,  
(Boulder Colorado, Westview Press, 1994).

U.S. Department of the Army. Force XXI Operations. TRADOC Pam  
525-5. Fort Monroe, Virginia: Headquarters, US Army Training  
and Doctrine Command, 1 August 1994.

U.S. Department of the Army. Information Operations. Field  
Manual 100-6. Washington D.C.: US Department of the Army, 27  
August 1996.

U.S. Department of the Army. Information Operations Pamphlet.  
Washington D.C.: US Department of the Army, (1998).

U.S. Joint Chiefs of Staff, and the National Defense University,  
Information Warfare: Legal, Regulatory, Policy and  
Organizational Considerations for Assurance, 2<sup>nd</sup> Edition  
(Washington: US Government Printing Office)

U.S. Joint Chiefs of Staff, Joint Doctrine for Information  
Operations. Joint Pub 3-13. Washington D.C.: US Joint Chiefs  
of Staff, 9 October 1998.

U.S. Joint Chiefs of Staff. Joint Vision 2010. Washington D.C.:  
US Joint Chiefs of Staff, July 1996.

U.S. Joint Chiefs of Staff. Concept for Future Joint Operations;  
Expanding Joint Vision 2010. Washington D.C.: US Joint  
Chiefs of Staff, May 1997.

Verton, Daniel M., "DOD preps office for cyberdefense", Federal  
Computer Week, 13 July 1998 Available from  
<<http://www.fcw.co.../fcw-newscyper-7-13-98.html>>; Internet  
accessed 30 Dec 1998.

Wilde, Andy, "Update: Information Operations." A Common Perspective, US Atlantic Command Joint Warfighting Center Newsletter, (Oct 1998):7-10.